02-20-04

Application No.: 10/718417

Title: Date Rights Management of Digital Information In A Portable Software Permission Wrapper

Inventor(s): David Duncan et al

Filing Date: November 20, 2003

Attorney Docket No.: e20031101

INFORMATION DISCLOSURE STATEMENT

Dear Sir/Madam:

This Information Disclosure Statement is filed pursuant to 37 CFR 1.97 and 1.98. This Information Disclosure Statement is timely in that it is being filed within three months of the filing date of the original national application. Enclosed herewith is USPTO Form SB/08A and 08B listing the patents, patent application and publications for consideration by the Patent Office and a copy of each patent, patent application and publication.

U.S. Patent Nos. 6,185,683; 6,339,825 and 6,449,721.

U.S. Patent No. 6,185,683 discloses electronic appliances such as computers to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. Distributed and other operating systems, environments and architectures, such as, for example, those using tamper-resistant hardware-based processors, may establish security at each node. These techniques may be used to support an all-electronic information distribution, for example, utilizing the "electronic highway."

A VDE is a "black box" container for protecting digital content. The VDE can exert transactional control over user rights using nodes (SPUs), and nodal transactions to convey rights from first to second, from second to third, and from first to third.

sensitive content, and depending on their permission, may or may not be able to save or store the data to their local PC.

Content servers provide a straightforward mechanism for protecting content. However, their weakness is based on the model wherein sensitive business information is only protected when it is physically on the server. Once the data is allowed off of the server, the data is not controlled unless another security mechanism is used, such as a permission wrapper. Another weakness in the content server model is that both the sender and the recipient must have online access to the content server. This can be a significant issue for remote or traveling users, or users that do not have shared IT infrastructure and a direct network path to the server. As a result, most content servers are used predominately as an "inside" enterprise information protection solution since they are not an effective mechanism for sharing sensitive data outside the enterprise.

U.S. Patent No. 6,499,106 and Patent Application No. 2001/0042043A1.

U. S. Patent No. 6,499,106 discloses a central control system for distributing information recorded on a fixed media 120, including a central access control system 100 and any number of information access systems connected to the central access control system 100 and uniquely identifying the fixed media 200. The central access control system 100 provides a decryption key to access the fixed media based on disc identification information 200.

The present invention does not rely on a unique identifier on the fixed media to grant access to the protected information. Rather it utilizes the secure data storage application software which dictates what is necessary in order to gain access to the archive, whether it is password, a product key and/or machine identifier and/or other access means to grant access to the protected information and further dictates what the user can do with the secure content with of without access to a central access control.

U. S Patent Application Publication No. 2001/0042043A1 discloses the use of rights management in association with removable or portable storage medium (CDs and DVDs). See paragraphs 0069, 0070 an 0071, 0183 to 0290.

These two references are relevant to the claims of the present invention that relate to removable media.

U.S. Patent Nos. 6,112,181; 6,412,070 and 6,519,647.

U. S. Patent No. 6,112,181 is directed to systems and methods for matching, selecting, narrowcasting, and/or classifying based on rights management and/or other information. In particular, is discloses an example of matching and classification utility system 900 including an object classifier 902, a user classifier 904 and a matching engine 906. Object classifier 902 receives information about objects and uses that information to classify those objects into groups based on the qualities or characteristics of the objects. User classifier 904 classifies and /or selects people based at least in part on these inputs.

VDE allows the owners and distributors of electronic digital information to reliably bill, for, and securely control, audit, and budget the use of, electronic information. It can reliably detect and monitor the use of commercial information products. VDE uses a wide variety of different electronic information delivery means: including, for example, digital networks, digital broadcast, and physical storage media such as optical and magnetic disks. VDE can be used by major network providers, hardware manufacturers, owners of electronic information, providers of such information, and clearinghouses that gather usage information regarding, and bill for the use of, electronic information.

Specifically, this preference discloses a system having secure electronic delivery means 4060 having an electronic container 302 containing an object 300 (See Figs. 5A and 5B) or a governed item 4054 (at least partially encrypted digital information) and having a first secure container rule, received from a third apparatus (trusted go-between 4700) different from a second apparatus, at least in part governing an aspect of access to or use of said first secure container 302 containing a governed item or object 300. Additionally, hardware or software is used for receiving and opening the secure containers. Thus, this patent teaches that the secure container requires a trusted electronic go-between 4700 is needed in order to redistribute the governed item. The container does not have the capacity to contain both the digital information to be protected and the access controls which govern access to the information. This reference teaches that a third apparatus is necessary in order to provide the necessary access to the content.

U.S. Patent No. 6,339,825 discloses system and method wherein digital information is encrypted in order to protect it from unauthorized access. This invention is one attempt to solve the problem of transmitting digital information from a central location to subscribers 104 who are remote to the content provider 102. The encrypted digital information of this invention does have any ability to be viewed without access to a remote/key server 106, 206 which provides the decryption key and software necessary to access the digital information and teaches to destroy the digital information once rendered.

U. S. Patent No. 6,449,721 discloses a method of controlling distribution of encrypted digital information 112 wherein a user 116, receives at their location from a key/remote server 106, 206 a user code and the encrypted information such that the decryption key is destroyed immediately after decrypting or rendering the information and defending the decryption key from capture at the user location. This patent is related to the '825 patent and is concerned with the distribution of digital information to subscribers and the prevention of unauthorized use of the digital information by persons who "steal" the decryption key and gain access to the distributed digital information.

Each of these patents is an example of a content server which is used to host sensitive information. The Content Server is used to store all sensitive information for the business. If a user wants to send sensitive content to a recipient, it is first sent and stored on the content server. The recipient then logs-in to the content server to access the

Matching engine 906 matches things up with things, things with people and/or people with people based on the classification inputs. U.S. Patent Applications 2003/0046244A1; 2003/0067948A1; and 2003/0067949A1 are pending divisional/continuation applications from the application into which the '181 patent issued.

U. S. Patent No. 6,412,070 discloses a system wherein a user 145 can dynamically create unique control access rights for one or more objects 125. The control access rights do not control access to data within objects 125, but control access to an operation, or action to be performed on or by object 125. It discloses the use of access-control list and access-control entries that identify a trusted application 140 and specifies permitted access rights for that trustee.

U. S. Patent No. 6,519,647 discloses a method and apparatus for synchronizing access control in a Web server wherein a plurality of security scenarios are defined and each scenario has one or more security setting associated with it. One or more of the security settings for a plurality of the access control mechanisms are automatically set when a security scenario is selected by the user. Thus, the security settings for a number of different access control mechanism can be set contemporaneously by selecting one security scenario.

These references are relevant to any claim relating to the use of templates to establish access to the secure content.

PUBLICATIONS

The paper entitled "Protection Techniques In Data Processing Systems To Meet User Data Security Needs" discuses data security: the protection of the information stored and referenced in data processing equipment. It states that there are four general categories into which protection techniques fall: physical protection, personnel practices, administrative procedures, and computer technology. Specifically it teaches to obtain identification of the user by one or more of their physical characteristics, but recognizes that identity verification is the more technologically feasible using passwords or personal information. This reference also discusses authorization, authentication, logging and journaling and cryptography. The present invention is mainly concerned with the personnel practices and administrative procedures.

The reference entitled "Information Systems Security" discusses the properties that a system should exhibit, those being integrity, auditability and controllability. It goes on to state that in order to achieve these properties, the system must exhibit functional controls on each domain's interface to protect the passage of information in the system from being compromised. The *identification* function identifies by some acceptable means the people, hardware, software and other resources available to a system. It implies only that a record exists in the system that associates an identifier with a defined user or resource. The *authentication* function provides the capability to verify the identified user or resource via a password, physical identification or appearance, or a unique reproducible behavior. The *authorization* function determines who is allowed to do what with a given

resource. The *delegation* function determines who my exercise or change the rules of authorization. Generally this is the system administrator. The *journaling* function provides a record of the use to the system and *surveillance* function requires that someone review the journals.

The reference entitled "Building a Secure Computer System" discusses the "multilevel security policy" which defines a structure of an access class and establishes the partial ordering relationship between access classes called dominates. This dominate relationship has two properties that make it a "lattice". This referenced introduces the concept of "trusted subjects" or "trusted users" as use in the present invention.

The reference entitled "Trusted Network Interpretation" discusses the need for a network security policy which is an access control policy having two primary components: mandatory and discretionary. The discretionary policy is for protecting the information being accessed based on the authorization of the users or groups of users, while the mandatory policy defines the set of distinct sensitivity levels of the information that is to be accessed. These policies can be applied to the level of secrecy of the information and/or to the data integrity. The policies then define what a user can do with the information, read only, write to, etc. This reference goes on to discuss the need for a record of identification and authentications as well as an audit record of what was done with the information.

No where in these references does it teach how to accomplish these functions, except the use of passwords or biometrics for authentication, but only that these functions are necessary in order to have a secure system.

Respectfully submitted,

J. Henry Muetterties
Reg. No. 30,301

Certification of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the Unites States Postal Service with sufficient postage as first class mail (Express Mail Label No. ER 540497627 US) in an envelope addressed to:

Commissioner of Patents
P. O. Box 1450
Alexandria, VA 22313-1450

on February 19, 2004.

J. Henry Muetterties
Reg. No. 30,301

Correspondence:

1. Information Disclosure Statement (5 pages)
2. Information Disclosure Statement By Applicant (Forms PTO/SB/08A and 08B).
3. Copy of each reference listed in Item 2.
4. Postcard

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	10/718417
Filing Date	November 20, 2003
First Named Inventor	David Duncan et al
Art Unit	
Examiner Name	
Attorney Docket Number	e20031101

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 6339825 B2	01-15-2002	Pensak et al	Col.1.ln 59 to
		US-			Col. 9 ln 29
		US- 6449721 B1	09-10-2002	Pensak et al	same
		US- 6185683 B1	02-06-2001	Ginter et al	Figs.5A,5B;Col 15,ln
		US-			31 to Col 48,ln51
		US- 6499106 B1	12-24-2002	Yaegashi e al	Col.10, ln 10 to
		US-			Col. 12, ln.61
		US- 2001/0042043 A1	11-15-2001	Shear et al	Paras 0069,0070 and
		US-			0290
		US- 6412070 B1	06-25-2002	Van Dyke et al	Col. 5,ln 50 to
		US-			Col.10, ln 24
		US- 6519647 B1	02-11-2003	Howard et al	Col. 5, ln 39 to
		US-			Col. 11, ln 12
		US- 6112181	08-29-2000	Shear et al	Col. 33, ln40-Col 64
		US-			,ln 47 and Col 70,
		US-			ln 50-Col 75, ln 61
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	10/718417
Filing Date	November 20, 2003
First Named Inventor	David Duncan et al
Art Unit	
Examiner Name	
Attorney Docket Number	e20031101

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		MORRIE GASSER, Building a Secure Computer System, 1988, pgs. 150 to 154, Van Nostrand Reinhold Comapny, New York, NY	
		ROYAL P. FISHER, Information Systems Security, 1984, pgs. 24 to 30, Prentice-Hall, Inc., Englewood Cliffs, NJ	
		BROADMAN, I.S, Protection Techniques in Data Processing Systems to Meet User data Security Needs in Tutorial on Computer Security and Integrity, 1977,	
		pgs. V-3 to V-7, IEEE Computer Society, Long Beach, CA	
		AUTHOR UNKNOWN, Trusted Network Interpretation, 31 July 1987, pgs. 32 to 37, National Computer Security Center, USA	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.